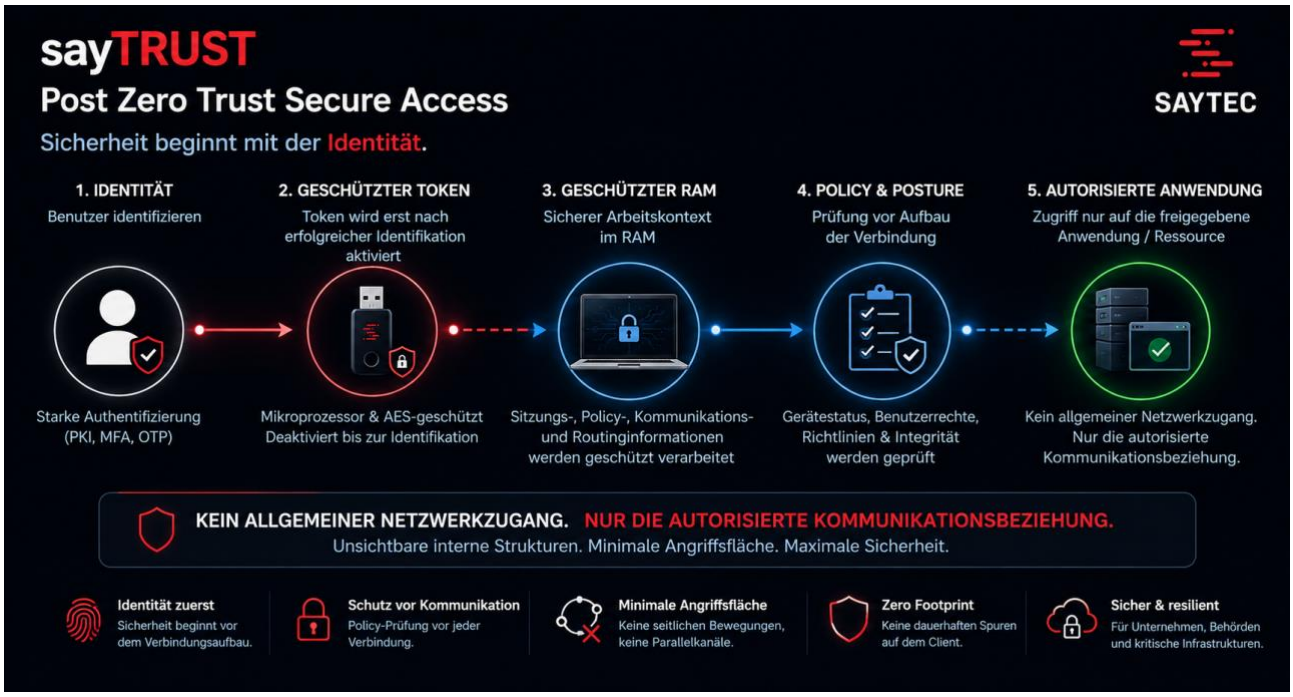
SAYTEC | SECURITY BY DESIGN

sayTRUST UZE – Post-Zero-Trust Secure Access und dedizierte Kommunikation

Universal Zero Trust Exchange: kontrollierter Zugriff auf Anwendungen, Daten, Maschinen und Standorte – ohne allgemeinen Netzwerkzugang.



Die Sicherheit beginnt mit der Identität des Nutzers – vor dem Tunnel, bevor die Kommunikation startet - vor der Freigabe einer Anwendung oder Sicherheits-umgebung.

Die Lösung auf einem Blick

sayTRUST UZE verbindet den zentralen UZE-Server mit hardware- oder softwarebasierten UZE-Clients. Freigegeben wird ausschließlich die jeweils autorisierte Kommunikationsbeziehung zu einer Anwendung, einem Dienst, einer Maschine oder einem definierten Standort. Der Benutzer erhält dabei keinen allgemeinen Zugriff auf das Unternehmensnetzwerk.

Die Sicherheitskette beginnt bei der eindeutigen Identifikation des Nutzers vor dem Rechner. Erst danach wird die geschützte Client-Umgebung aktiviert, Richtlinien und Sicherheitszustand geprüft und die konkret zugelassene Kommunikation aufgebaut.

Post Zero Trust bildet das gesamte sayTEC-Architekturmodell; sayTRUST UZE ist die technische Plattform, die dieses Prinzip umsetzt.

VPN verbindet. Zero Trust kontrolliert. Post Zero Trust isoliert die autorisierte Kommunikationsbeziehung und verlagert die Sicherheitsentscheidung konsequent vor den Kommunikationsaufbau.

Warum der Tunnel allein nicht genügt

Klassische VPN-Lösungen koppeln einen entfernten Rechner trotz Verschlüsselung technisch an ein Netzwerk oder einen Netzbereich. Wird der Client kompromittiert, kann diese Verbindung selbst zum Angriffsweg werden. Zero Trust und ZTNA verbessern die Kontrolle, sayTRUST UZE führt den Gedanken weiter: Es wird nicht mehr das Netzwerk geöffnet, sondern nur noch die autorisierte Kommunikationsbeziehung zu einer konkret freigegebenen Ressource – etwa zu einer Anwendung, einem Service, einem Maschinenzugriff oder einer Sprach- und Videokommunikation.

Die Sicherheitskette

	Sicherheitsstufe	Wirkung
1	Identifikation	Der berechtigte Nutzer wird vor Aktivierung der Kommunikation und Sicherheitsumgebung eindeutig überprüft.
2	UZE-Client	Der persönliche Hardware-Client oder der gerätegebundene Software-Client wird kontrolliert aktiviert und überwacht.
3	Geschützter RAM-Kontext	Sitzungs-, Policy-, Kommunikations- und Routinginformationen werden temporär und geschützt verarbeitet.
4	Policy und Posture	Berechtigungen, Zertifikate, Richtlinien und Sicherheitszustand werden vor der Kommunikation geprüft.
5	Autorisierter Exchange	Der UZE-Server vermittelt nur die ausdrücklich freigegebene Anwendung oder Kommunikationsbeziehung.

Interne und externe Arbeitsplätze werden nach demselben Prinzip geschützt

sayTRUST UZE ist nicht nur für Homeoffice und mobile Nutzer konzipiert. Auch interne Arbeitsplätze, private Geräte, Dienstleisterzugänge und getrennte Netzwerkbereiche können nach derselben Sicherheitslogik behandelt werden. Entscheidend ist das Ineinandergreifen mehrerer Sicherheitsböcke: Überprüfung der Identität, der verschlüsselte UZE-Client und die autorisierte Beziehung – nicht der Netzwerkstandort allein.

Dadurch bleiben Server und kritische Ressourcen gegenüber Endgeräten maximal abgeschirmt. Nicht autorisierte Systeme sind nicht sichtbar, nicht frei adressierbar und nicht direkt erreichbar.

Hardware- und Software-Clients

Hardwarebasierte und softwarebasierte UZE-Clients können innerhalb derselben Umgebung genutzt werden. Hardware-Clients sind portabel und besonders für hohe Schutzanforderungen geeignet; der Software-Client bezieht sich fest auf ein definiertes Gerät.

UZE-Client	Aktivierung / Plattform	Geeigneter Einsatz
UZE-Software-Client	Gerätegebunden	Definierte interne Umgebung oder feste Arbeitsplätze
UZE-Biometrie-Client	Biometrie/Passwort, AES-256	Portabler, biometrisch geschützter Fernzugriff
UZE-Mikroprozessor-Biometrie-Client	Biometrie, AES-256, Mikrocontroller	Besonders hohe Sicherheits-anforderungen. Portabel biometrisch geschützter Fernzugriff
UZE-USB-Client	USB-Flash	Definierte Nutzergruppen ohne Biometrie
UZE-USB-PIN-Code-Client	Code-Aktivierung, AES-256	Codegeschützter Fernzugriff

Skalierbare UZE-Serverplattform

Der UZE-Server ist als Serverbetriebssystem für vorhandene Hardware oder unterstützte virtuelle Umgebungen sowie als vorkonfigurierte physische Appliance verfügbar. Die Leistungsklassen Basic, Professional und Enterprise ermöglichen eine projektbezogene Dimensionierung.

Klasse	Betriebsform	Enthaltene Client-Lizenzen	Max. Verbindungen
Basic	Software oder Appliance	5	25
Professional	Software oder Appliance	5	250
Enterprise	Software oder Appliance	5	lizenzseitig unbegrenzt*

* Die technisch unterstützte Kapazität richtet sich nach der jeweils konkreten Plattformauslegung.

Hochverfügbarkeit ohne doppelte Client-Lizenzierung

Für hochverfügbare Installationen steht eine separate HA-Appliance mit integriertem HA-Serverbetriebssystem zur Verfügung. Sie übernimmt Lizenzumfang und Verbindungskapazität des zugeordneten UZE-Masters; die Client-Lizenzen müssen für das redundante System nicht erneut erworben werden.

UZE Plus für Maschinen, Server und Standorte

UZE Plus erweitert die Plattform um eine dedizierte Maschine-zu-Maschine- und Standort-zu-Standort Kommunikation. Bis zu zwölf Maschinen oder definierte Netze beziehungsweise Subnetze können angebunden werden. Auch hier wird kein entferntes Netzwerk pauschal angebunden; es kommunizieren nur die autorisierten Systeme und Beziehungen mit den jeweiligen Netzen.

Die UZE Plus Appliance Enterprise verbindet den personenbezogenen UZE-Client-Zugriff mit dedizierter Kommunikation zwischen Maschinen, Server, Netze und Standorte.

Nutzen und typische Einsatzfelder

- Eindeutige Identität als Ausgangspunkt der Sicherheitskette.
- Policy-, Posture- und Kommunikationsprüfung vor dem Aufbau einer Kommunikation und Beziehung.
- Anwendungsbezogener Zugriff ohne allgemeinen Netzwerkzugang.
- Zero-Footprint-Prinzip und geschützter temporärer RAM-Kontext.
- Einheitliches Sicherheitsmodell für interne und externe Arbeitsplätze.
- Kontrollierter Zugriff für Nutzer, Partner und Dienstleister.
- Dedizierte Kommunikation für Maschinen, Server, Netze und Standorte.
- Reduzierte Sichtbarkeit interner Strukturen und deutlich geringere Angriffsfläche.

Fazit

sayTRUST UZE verbindet Identität, Client-Aktivierung, geschützten Arbeitsspeicherkontext, Policy Enforcement, Posture-Prüfung, UZE-Server, Kommunikationskontrolle und Zero Footprint zu einer durchgängigen Post-Zero-Trust-Sicherheitsarchitektur.

Nicht das Netzwerk wird geöffnet – sondern ausschließlich die freigegebene Kommunikationsbeziehung zu einer bestimmten Anwendung